UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/976,447	10/12/2001	Takayuki Sato	04610.004001	3936

22511 7590 09/27/2005

OSHA LIANG L.L.P.
1221 MCKINNEY STREET
SUITE 2800
HOUSTON, TX 77010

EXAMINER	
LANIER, BENJAMIN E	
ART UNIT	**PAPER NUMBER**
2132	

DATE MAILED: 09/27/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/976,447	SATO, TAKAYUKI	
	Examiner	Art Unit	
	Benjamin E. Lanier	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-34* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-34* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *12 October 2001* is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date 3/03/02, 12/26/02
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 112

1. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

2. Claims 9, 10, 15, 25 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

3. Claims 9, 10, 15, 25 recite "...notify a predetermined managing computer of the source IP address of the external apparatus which is determined as the apparatus to be responded to" renders the claim vague and indefinite because it creates a contradictory situation in that the limitation requires notification to be send to an apparatus that is not to be responded to. For the purposes of examination claim 9 will be treated as having a notification sent to the external apparatus.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. Claims 1, 3, 5, 6, 7, 9, 11, 12, 14, 16, 18, 20-22, 24, 26, 28-31, 33 are rejected under 35 U.S.C. 102(e) as being anticipated by Kalajan, U.S. Patent No. 6,205,156. Referring to claim 1,

Kalajan discloses an access control system wherein a communication data path is established between a first client and a HTTP server over the Internet (Col. 3, lines 43-45, 55-56), which meets the limitation of packets being transmitted/received between a plurality of computers and being structured to be controllable by an external apparatus based on a TCP/IP protocol. In order to establish the communication path the first client must validate itself to the server using a form of one-time validation (Col. 3, line 64 – Col. 4, line 4). Once the first client is validated, the IP address (Col. 3, lines 50-51) of the first client is considered a validated network address by the server and the client validation system of the server establishes the access-controlled communications path by instructing firewall to allow packets from the first client (Col. 4, lines 22-31), which meets the limitation of extracting and storing a source IP address included in a packet which is transmitted from an external apparatus when an access from the external apparatus is authenticated through execution of the TCP/IP protocol. During communications over the access-controlled communications path, the firewall allows only data packets from validated network addresses to pass through to access-controlled port. Each communications or data packet from a client typically includes information indicating the source network address of the packet. This information can be used to determine whether or not the server will accept the packets or communicate with the source of incoming communications (Col. 4, lines 33-41), which meets the limitation of judging when an access from an external apparatus occurs thereafter, whether or not a source IP address of the external apparatus giving the access is identical with the stored source IP address, permitting communication thereafter between the external apparatus having the source IP address identical with the stored transmitting end IP

address and the intelligent interconnecting device only when the source IP address of the external apparatus is judged to be identical with the stored source IP address.

Referring to claim 3, while Kalajan discloses that if a connection with a client is blocked, no information regarding the blocking of the connection will be sent to the client, the teaching still meets the limitation of notifying an authenticated managing computer of the source IP address of the external apparatus which is judged to be nonidentical when the source IP address is judged to be nonidentical with the stored source IP address because MPEP 2123 discloses:

> "The use of patents as references is not limited to what the patentees describe as their own inventions or to the problems with which they are concerned. They are part of the literature of the art, relevant for all they contain." In re Heck, 699 F.2d 1331, 1332-33, 216 USPQ 1038, 1039 (Fed. Cir. 1983) (quoting In re Lemelson, 397 F.2d 1006, 1009, 158 USPQ 275, 277 (CCPA 1968)).
>
> A reference may be relied upon for all that it would have reasonably suggested to one having ordinary skill the art, including nonpreferred embodiments. Merck & Co. v. Biocraft Laboratories, 874 F.2d 804, 10 USPQ2d 1843 (Fed. Cir.), cert. denied, 493 U.S. 975 (1989). See also Celeritas Technologies Ltd. v. Rockwell International Corp., 150 F.3d 1354, 1361, 47 USPQ2d 1516, 1522-23 (Fed. Cir. 1998) (The court held that the prior art anticipated the claims even though it taught away from the claimed invention. "The fact that a modem with a single carrier data signal is shown to be less than optimal does not vitiate the fact that it is disclosed.").
>
> Disclosed examples and preferred embodiments do not constitute a teaching away from a broader disclosure or nonpreferred embodiments. In re Susi, 440 F.2d 442, 169 USPQ 423 (CCPA 1971). "A known or obvious composition does not become patentable simply because it has been described as somewhat inferior to some other product for the same use." In re Gurley, 27 F.3d 551, 554, 31 USPQ2d 1130, 1132 (Fed. Cir. 1994) (The invention was directed to an epoxy impregnated fiber-reinforced printed circuit material. The applied prior art reference taught a printed circuit material similar to that of the claims but impregnated with polyester-imide resin instead of epoxy. The reference, however, disclosed that epoxy was known for this use, but that epoxy impregnated circuit boards have "relatively acceptable dimensional stability" and "some degree of flexibility," but are inferior to circuit boards impregnated with polyester-imide resins. The court upheld the rejection concluding that applicant's argument that the reference teaches away from using epoxy was insufficient to overcome the rejection since "Gurley asserted no discovery beyond what was known in the art." 27 F.3d at 554, 31 USPQ2d at 1132.).

Referring to claim 5, Kalajan discloses that the communication path is maintained between the client and the server for a predetermined period of time. The communication path is terminating at the end of the period of time and the client must be revalidated to resume the access-controlled communication path (Col. 4, line 66 – Col. 5, line 10), which meets the limitation of judging whether or not the source IP address which is judged to be identical with the stored source IP address is within a valid period set in advance when the source IP address is judged to be identical with the stored source IP address, permitting communication thereafter between the external apparatus having the source IP address which is judged to be within the valid period and the intelligent interconnecting device only when the source IP address of the external apparatus is judged to be within the valid period.

Referring to claims 6, 11, Kalajan discloses an access control system wherein a communication data path is established between a first client and a HTTP server over the Internet (Col. 3, lines 43-45, 55-56), which meets the limitation of packets being transmitted/received between a plurality of computers and being structured to be controllable by an external apparatus based on a TCP/IP protocol. In order to establish the communication path the first client must validate itself to the server using a one-time password (Col. 3, line 64 – Col. 4, line 4), which meets the limitation of a first step of causing the intelligent interconnecting device to judge whether or not a first access to the intelligent interconnecting device from outside has occurred, a second step of causing the intelligent interconnecting device to carry out authentication processing by using a user identifier and a password based on the TCP/IP protocol when it is judged in said first step that the first access from outside has occurred, a third step of

causing the intelligent interconnecting device to judge after the authentication processing in said second step whether or not authentication is given, a fourth step of determining an authenticated external apparatus as an apparatus to be responded to thereafter by the intelligent interconnecting device and causing the intelligent interconnecting device to judge whether or not this access is the first access, when it is judged in said third step that the authentication is given. Once the first client is validated, the IP address (Col. 3, lines 50-51) of the first client is considered a validated network address by the server and the client validation system of the server establishes the access-controlled communications path by instructing firewall to allow packets from the first client (Col. 4, lines 22-31), which meets the limitation of a fifth step of causing the intelligent interconnecting device to extract and store a source IP address included in a packet which is received from an external apparatus in the authentication processing when this access of the external apparatus is judged to be the first access in said fourth step. If the client is not authenticated the client is not responded to (Col. 4, lines 46-50), which meets the limitation of a sixth step of determining the external apparatus as an apparatus not to be responded to thereafter by the intelligent interconnecting device when the external apparatus is judged not to be authenticated in said third step. During communications over the access-controlled communications path, the firewall allows only data packets from validated network addresses to pass through to access-controlled port. Each communications or data packet from a client typically includes information indicating the source network address of the packet. This information can be used to determine whether or not the server will accept the packets or communicate with the source of incoming communications (Col. 4, lines 33-41), which meets the limitation of a seventh step of causing the intelligent interconnecting device to judge whether

or not a source IP address of the external apparatus giving the access thereto is identical with the stored source IP address when this access is judged not to be the first access in said first step, an eighth step of determining the external apparatus whose source IP address is judged to be identical with the stored source IP address as an apparatus to be responded to thereafter by the intelligent interconnecting device and causing the intelligent interconnecting device to process the steps beginning from said second step, when the source IP address of the external apparatus is judged to be identical with the stored source IP address in said seventh step. If the client network address does not match then the client is not responded to (Col. 4, lines 46-50), which meets the limitation of a ninth step of determining the external apparatus whose source IP address is judged to be nonidentical with the stored source IP address as an apparatus not to be responded to thereafter by the intelligent interconnecting device when the source IP address of the external apparatus is judged to be nonidentical with the stored source IP address in said seventh step.

Referring to claims 7, 22, 31, Kalajan discloses an access control system wherein a communication data path is established between a first client and a HTTP server over the Internet (Col. 3, lines 43-45, 55-56), which meets the limitation of a LAN trunk line interfacing section having an interface function with a LAN trunk line, packets being transmitted/received between a plurality of computers and being structured to be controllable by an external apparatus based on a TCP/IP protocol. In order to establish the communication path the first client must validate itself to the server using a one-time password (Col. 3, line 64 – Col. 4, line 4), which meets the limitation of a first step of causing the intelligent interconnecting device to judge whether or not a first access to the intelligent interconnecting device from outside has occurred, a

second step of causing the intelligent interconnecting device to carry out authentication processing by using a user identifier and a password based on the TCP/IP protocol when it is judged in said first step that the first access from outside has occurred, a third step of causing the intelligent interconnecting device to judge after the authentication processing in said second step whether or not authentication is given, a fourth step of determining an authenticated external apparatus as an apparatus to be responded to thereafter by the intelligent interconnecting device and causing the intelligent interconnecting device to judge whether or not this access is the first access, when it is judged in said third step that the authentication is given. Once the first client is validated, the IP address (Col. 3, lines 50-51) of the first client is considered a validated network address by the server and the client validation system of the server establishes the access-controlled communications path by instructing firewall to allow packets from the first client (Col. 4, lines 22-31), which meets the limitation of a storage section for storing a program and data therein, a fifth step of causing the intelligent interconnecting device to extract and store a source IP address included in a packet which is received from an external apparatus in the authentication processing when this access of the external apparatus is judged to be the first access in said fourth step. If the client is not authenticated the client is not responded to (Col. 4, lines 46-50), which meets the limitation of a sixth step of determining the external apparatus as an apparatus not to be responded to thereafter by the intelligent interconnecting device when the external apparatus is judged not to be authenticated in said third step. During communications over the access-controlled communications path, the firewall allows only data packets from validated network addresses to pass through to access-controlled port, which meets the limitation of a port interfacing section having an interface function with a terminal connected thereto. Each

communications or data packet from a client typically includes information indicating the source network address of the packet. This information can be used to determine whether or not the server will accept the packets or communicate with the source of incoming communications (Col. 4, lines 33-41), which meets the limitation of a central controlling section for controlling operations of said LAN trunk line interfacing section, said port interfacing section, and said storage section, a seventh step of causing the intelligent interconnecting device to judge whether or not a source IP address of the external apparatus giving the access thereto is identical with the stored source IP address when this access is judged not to be the first access in said first step. The communication path is maintained between the client and the server for a predetermined period of time. The communication path is terminating at the end of the period of time and the client must be revalidated to resume the access-controlled communication path (Col. 4, line 66 – Col. 5, line 10), which meets the limitation of an eighth step of causing the intelligent interconnecting device to judge whether or not the source IP address is within a predetermined valid period when the source IP address of the external apparatus is judged to be identical with the stored source IP address in said seventh step, an ninth step of determining the external apparatus whose source IP address is judged to be the predetermined valid period as an apparatus to be responded to thereafter by the intelligent interconnecting device and causing the intelligent interconnecting device to execute the steps beginning from said second step, when the source IP address of the external apparatus is judged to be within the predetermined valid period in said eighth step. If the client network address does not match then the client is not responded to (Col. 4, lines 46-50), which meets the limitation of a tenth step of determining the external apparatus whose source IP address is judged to be nonidentical or is judged to be no within the

predetermined valid period as an apparatus not to be responded to thereafter by the intelligent interconnecting device when the source IP address of the external apparatus is judged to be nonidentical with the stored source IP address in said seventh step or is judged to be not within the predetermined valid period in said eighth step.

Referring to claims 9, 12, 14, 21, 24, 30, 33, Kalajan discloses an access control system wherein a communication data path is established between a first client and a HTTP server over the Internet (Col. 3, lines 43-45, 55-56), which meets the limitation of a LAN trunk link interfacing section having an interface function with a LAN trunk line, packets being transmitted/received between a plurality of computers and being structured to be controllable by an external apparatus based on a TCP/IP protocol. In order to establish the communication path the first client must validate itself to the server using a one-time password (Col. 3, line 64 – Col. 4, line 4), which meets the limitation of a first step of causing the intelligent interconnecting device to judge whether or not a first access to the intelligent interconnecting device from outside has occurred, a second step of causing the intelligent interconnecting device to carry out authentication processing by using a user identifier and a password based on the TCP/IP protocol when it is judged in said first step that the first access from outside has occurred, a third step of causing the intelligent interconnecting device to judge after the authentication processing in said second step whether or not authentication is given, a fourth step of determining an authenticated external apparatus as an apparatus to be responded to thereafter by the intelligent interconnecting device and causing the intelligent interconnecting device to judge whether or not this access is the first access, when it is judged in said third step that the authentication is given. Once the first client is validated, the IP address (Col. 3, lines 50-51) of the first client is considered a validated

network address by the server and the client validation system of the server establishes the access-controlled communications path by instructing firewall to allow packets from the first client (Col. 4, lines 22-31), which meets the limitation of a storage section for storing a program and data therein, a fifth step of causing the intelligent interconnecting device to extract and store a source IP address included in a packet which is received from an external apparatus in the authentication processing when this access of the external apparatus is judged to be the first access in said fourth step. If the client is not authenticated the client is not responded to (Col. 4, lines 46-50), which meets the limitation of a sixth step of determining the external apparatus as an apparatus not to be responded to thereafter by the intelligent interconnecting device when the external apparatus is judged not to be authenticated in said third step. During communications over the access-controlled communications path, the firewall allows only data packets from validated network addresses to pass through to access-controlled port, which meets the limitation of a port interfacing section having an interface function with a terminal connected thereto. Each communications or data packet from a client typically includes information indicating the source network address of the packet. This information can be used to determine whether or not the server will accept the packets or communicate with the source of incoming communications (Col. 4, lines 33-41), which meets the limitation of a central controlling section for controlling operations of said LAN trunk line interfacing section, said port interfacing section, and said storage section, a seventh step of causing the intelligent interconnecting device to judge whether or not a source IP address of the external apparatus giving the access thereto is identical with the stored source IP address when this access is judged not to be the first access in said first step. The communication path is maintained between the client and the server for a predetermined

period of time. The communication path is terminating at the end of the period of time and the client must be revalidated to resume the access-controlled communication path (Col. 4, line 66 – Col. 5, line 10), which meets the limitation of an eighth step of causing the intelligent interconnecting device to judge whether or not the source IP address is within a predetermined valid period when the source IP address of the external apparatus is judged to be identical with the stored source IP address in said seventh step, an ninth step of determining the external apparatus whose source IP address is judged to be the predetermined valid period as an apparatus to be responded to thereafter by the intelligent interconnecting device and causing the intelligent interconnecting device to execute the steps beginning from said second step, when the source IP address of the external apparatus is judged to be within the predetermined valid period in said eighth step. If the client network address does not match then the client is not responded to (Col. 4, lines 46-50), which meets the limitation of a tenth step of determining the external apparatus whose source IP address is judged to be nonidentical or is judged to be no within the predetermined valid period as an apparatus not to be responded to thereafter by the intelligent interconnecting device when the source IP address of the external apparatus is judged to be nonidentical with the stored source IP address in said seventh step or is judged to be not within the predetermined valid period in said eighth step. While Kalajan discloses that if a connection with a client is blocked, no information regarding the blocking of the connection will be sent to the client, the teaching still meets the limitation of notifying an authenticated managing computer of the source IP address of the external apparatus which is judged to be nonidentical when the source IP address is judged to be nonidentical with the stored source IP address for the same reasoning mentioned above.

Referring to claims 16, 26, Kalajan discloses an access control system wherein a communication data path is established between a first client and a HTTP server over the Internet (Col. 3, lines 43-45, 55-56), which meets the limitation of a LAN trunk line interfacing section having an interface function with a LAN trunk line, packets being transmitted/received between a plurality of computers and being structured to be controllable by an external apparatus based on a TCP/IP protocol. In order to establish the communication path the first client must validate itself to the server using a form of one-time validation (Col. 3, line 64 – Col. 4, line 4). Once the first client is validated, the IP address (Col. 3, lines 50-51) of the first client is considered a validated network address by the server and the client validation system of the server establishes the access-controlled communications path by instructing firewall to allow packets from the first client (Col. 4, lines 22-31), which meets the limitation of a storage section for storing a program and data therein, extracting and storing a source IP address included in a packet which is transmitted from an external apparatus and stored in said storage section when an access from the external apparatus is authenticated through execution of the TCP/IP protocol. During communications over the access-controlled communications path, the firewall allows only data packets from validated network addresses to pass through to access-controlled port, which meets the limitation of a port interfacing section having an interface function with a terminal connected thereto. Each communications or data packet from a client typically includes information indicating the source network address of the packet. This information can be used to determine whether or not the server will accept the packets or communicate with the source of incoming communications (Col. 4, lines 33-41), which meets the limitation of a central controlling section for controlling operations of said LAN trunk line interfacing section, said port

interfacing section and said storage section, judging when an access from an external apparatus occurs thereafter, whether or not a source IP address of the external apparatus giving the access is identical with the stored source IP address, permitting communication thereafter between the external apparatus having the source IP address identical with the stored transmitting end IP address and the intelligent interconnecting device only when the source IP address of the external apparatus is judged to be identical with the stored source IP address.

Referring to claims 18, 28, while Kalajan discloses that if a connection with a client is blocked, no information regarding the blocking of the connection will be sent to the client, the teaching still meets the limitation of notifying an authenticated managing computer of the source IP address of the external apparatus which is judged to be nonidentical when the source IP address is judged to be nonidentical with the stored source IP address for the reasons state above.

Referring to claims 20, 29, Kalajan discloses that the communication path is maintained between the client and the server for a predetermined period of time. The communication path is terminating at the end of the period of time and the client must be revalidated to resume the access-controlled communication path (Col. 4, line 66 – Col. 5, line 10), which meets the limitation of judging whether or not the source IP address which is judged to be identical with the stored source IP address is within a valid period set in advance when the source IP address is judged to be identical with the stored source IP address, permitting communication thereafter between the external apparatus having the source IP address which is judged to be within the valid period and the intelligent interconnecting device only when the source IP address of the external apparatus is judged to be within the valid period.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

8. Claims 2, 4, 8, 10, 13, 15, 17, 19, 23, 25, 27, 32, 34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kalajan, U.S. Patent No. 6,205,156, in view of Barrett, U.S. Patent No. 6,832,321. Referring to claims 2, 17, 27, Kalajan discloses an access control system wherein a communication data path is established between a first client and a HTTP server over the Internet (Col. 3, lines 43-45, 55-56). Each communications or data packet from a client typically includes information indicating the source network address of the packet. This information can be used to determine whether or not the server will accept the packets or communicate with the source of incoming communications (Col. 4, lines 33-41). Kalajan does not disclose that the server contains a list of block source IP addresses. Barrett discloses a network access server having a firewall wherein the access server maintains a list of allowed IP addresses and blocked IP addresses (Col. 9, lines 32-37). It would have been obvious to one of ordinary skill in the art at the time the invention was made to include a list of blocked IP address is the access control

system of Kalajan in order to specify that inbound connections with certain source addresses should be blocked as taught in Barrett (Col. 9, lines 51-54).

Referring to claims 4, 19, 25, 34, while Kalajan discloses that if a connection with a client is blocked, no information regarding the blocking of the connection will be sent to the client, the teaching still meets the limitation of notifying an authenticated managing computer of the source IP address of the external apparatus which is judged to be nonidentical when the source IP address is judged to be nonidentical with the stored source IP address for the same reasoning mentioned above.

Referring to claims 8, 13, 23, 32, Kalajan discloses an access control system wherein a communication data path is established between a first client and a HTTP server over the Internet (Col. 3, lines 43-45, 55-56), which meets the limitation of a LAN trunk line interfacing section having an interface function with a LAN trunk line, packets being transmitted/received between a plurality of computers and being structured to be controllable by an external apparatus based on a TCP/IP protocol. In order to establish the communication path the first client must validate itself to the server using a one-time password (Col. 3, line 64 – Col. 4, line 4), which meets the limitation of a first step of causing the intelligent interconnecting device to judge whether or not a first access to the intelligent interconnecting device from outside has occurred, a second step of causing the intelligent interconnecting device to carry out authentication processing by using a user identifier and a password based on the TCP/IP protocol when it is judged in said first step that the first access from outside has occurred, a third step of causing the intelligent interconnecting device to judge after the authentication processing in said second step whether or not authentication is given, a fourth step of determining an authenticated external

apparatus as an apparatus to be responded to thereafter by the intelligent interconnecting device and causing the intelligent interconnecting device to judge whether or not this access is the first access, when it is judged in said third step that the authentication is given. Once the first client is validated, the IP address (Col. 3, lines 50-51) of the first client is considered a validated network address by the server and the client validation system of the server establishes the access-controlled communications path by instructing firewall to allow packets from the first client (Col. 4, lines 22-31), which meets the limitation of a storage section for storing a program and data therein, a fifth step of causing the intelligent interconnecting device to extract and store a source IP address included in a packet which is received from an external apparatus in the authentication processing when this access of the external apparatus is judged to be the first access in said fourth step. If the client is not authenticated the client is not responded to (Col. 4, lines 46-50), which meets the limitation of a sixth step of determining the external apparatus as an apparatus not to be responded to thereafter by the intelligent interconnecting device when the external apparatus is judged not to be authenticated in said third step. During communications over the access-controlled communications path, the firewall allows only data packets from validated network addresses to pass through to access-controlled port, which meets the limitation of a port interfacing section having an interface function with a terminal connected thereto. Each communications or data packet from a client typically includes information indicating the source network address of the packet. This information can be used to determine whether or not the server will accept the packets or communicate with the source of incoming communications (Col. 4, lines 33-41), which meets the limitation of a central controlling section for controlling operations of said LAN trunk line interfacing section, said port interfacing section, and said

storage section, a seventh step of causing the intelligent interconnecting device to judge whether or not a source IP address of the external apparatus giving the access thereto is identical with the stored source IP address when this access is judged not to be the first access in said first step. The communication path is maintained between the client and the server for a predetermined period of time. The communication path is terminating at the end of the period of time and the client must be revalidated to resume the access-controlled communication path (Col. 4, line 66 – Col. 5, line 10), which meets the limitation of an eighth step of causing the intelligent interconnecting device to judge whether or not the source IP address is within a predetermined valid period when the source IP address of the external apparatus is judged to be identical with the stored source IP address in said seventh step, an ninth step of determining the external apparatus whose source IP address is judged to be the predetermined valid period as an apparatus to be responded to thereafter by the intelligent interconnecting device and causing the intelligent interconnecting device to execute the steps beginning from said second step, when the source IP address of the external apparatus is judged to be within the predetermined valid period in said eighth step. If the client network address does not match then the client is not responded to (Col. 4, lines 46-50), which meets the limitation of a tenth step of determining the external apparatus whose source IP address is judged to be nonidentical or is judged to be no within the predetermined valid period as an apparatus not to be responded to thereafter by the intelligent interconnecting device when the source IP address of the external apparatus is judged to be nonidentical with the stored source IP address in said seventh step or is judged to be not within the predetermined valid period in said eighth step. While Kalajan discloses that if a connection with a client is blocked, no information regarding the blocking of the connection will be sent to

the client, the teaching still meets the limitation of notifying an authenticated managing computer of the source IP address of the external apparatus which is judged to be nonidentical when the source IP address is judged to be nonidentical with the stored source IP address for the same reasoning mentioned above. Kalajan does not disclose that the server contains a list of block source IP addresses. Barrett discloses a network access server having a firewall wherein the access server maintains a list of allowed IP addresses and blocked IP addresses (Col. 9, lines 32-37). It would have been obvious to one of ordinary skill in the art at the time the invention was made to include a list of blocked IP address is the access control system of Kalajan in order to specify that inbound connections with certain source addresses should be blocked as taught in Barrett (Col. 9, lines 51-54).

Referring to claims 10, 15, while Kalajan discloses that if a connection with a client is blocked, no information regarding the blocking of the connection will be sent to the client, the teaching still meets the limitation of notifying an authenticated managing computer of the source IP address of the external apparatus which is judged to be nonidentical when the source IP address is judged to be nonidentical with the stored source IP address for the same reasoning mentioned above.

Conclusion

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Benjamin E. Lanier whose telephone number is 571-272-3805. The examiner can normally be reached on M-Th0 7:30am-5:00pm, F 7:30am-4pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Benjamin E. Lanier

GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100